1 Static Semantics

$\boxed{\Theta; \Delta; \Gamma \vdash e : t}$ Typing rules for expressions

$$\frac{}{\Theta; \Delta; \cdot, x : t \vdash x : t} \quad \textsc{Ty\_Var\_Lin}$$

$$\frac{x : t \in \Delta}{\Theta; \Delta; \cdot \vdash x : t} \quad \textsc{Ty\_Var}$$

$$\frac{\begin{array}{l}\Theta; \Delta; \Gamma \vdash e : t \\ \Theta; \Delta; \Gamma', x : t \vdash e' : t'\end{array}}{\Theta; \Delta; \Gamma, \Gamma' \vdash \mathbf{let}\, x = e\, \mathbf{in}\, e' : t'} \quad \textsc{Ty\_Let}$$

$$\frac{}{\Theta; \Delta; \cdot \vdash () : \mathbf{unit}} \quad \textsc{Ty\_Unit\_Intro}$$

$$\frac{\begin{array}{l}\Theta; \Delta; \Gamma \vdash e : \mathbf{unit} \\ \Theta; \Delta; \Gamma' \vdash e' : t\end{array}}{\Theta; \Delta; \Gamma, \Gamma' \vdash \mathbf{let}\, () = e\, \mathbf{in}\, e' : t} \quad \textsc{Ty\_Unit\_Elim}$$

$$\frac{}{\Theta; \Delta; \cdot \vdash \mathbf{true} : \mathbf{bool}} \quad \textsc{Ty\_Bool\_True}$$

$$\frac{}{\Theta; \Delta; \cdot \vdash \mathbf{false} : \mathbf{bool}} \quad \textsc{Ty\_Bool\_False}$$

$$\frac{\begin{array}{l}\Theta; \Delta; \Gamma \vdash e : !\mathbf{bool} \\ \Theta; \Delta; \Gamma' \vdash e_1 : t' \\ \Theta; \Delta; \Gamma' \vdash e_2 : t'\end{array}}{\Theta; \Delta; \Gamma, \Gamma' \vdash \mathbf{if}\, e\, \mathbf{then}\, e_1\, \mathbf{else}\, e_2 : t} \quad \textsc{Ty\_Bool\_Elim}$$

$$\frac{}{\Theta; \Delta; \cdot \vdash k : \mathbf{int}} \quad \textsc{Ty\_Int\_Intro}$$

$$\frac{}{\Theta; \Delta; \cdot \vdash el : \mathbf{elt}} \quad \textsc{Ty\_Elt\_Intro}$$

$$\frac{\begin{array}{l}\Theta; \Delta; \cdot \vdash v : t \\ v \neq l\end{array}}{\Theta; \Delta; \cdot \vdash \mathbf{Many}\, v : !t} \quad \textsc{Ty\_Bang\_Intro}$$

$$\frac{\begin{array}{l}\Theta; \Delta; \Gamma \vdash e : !t \\ \Theta; \Delta, x : t; \Gamma' \vdash e' : t'\end{array}}{\Theta; \Delta; \Gamma, \Gamma' \vdash \mathbf{let}\, \mathbf{Many}\, x = e\, \mathbf{in}\, e' : t'} \quad \textsc{Ty\_Bang\_Elim}$$

$$\frac{\begin{array}{l}\Theta; \Delta; \Gamma \vdash e : t \\ \Theta; \Delta; \Gamma' \vdash e' : t'\end{array}}{\Theta; \Delta; \Gamma, \Gamma' \vdash (e, e') : t \otimes t'} \quad \textsc{Ty\_Pair\_Intro}$$

$$\frac{\begin{array}{l}\Theta; \Delta; \Gamma \vdash e_{12} : t_1 \otimes t_2 \\ \Theta; \Delta; \Gamma', a : t_1, b : t_2 \vdash e : t\end{array}}{\Theta; \Delta; \Gamma, \Gamma' \vdash \mathbf{let}\, (a, b) = e_{12}\, \mathbf{in}\, e : t} \quad \textsc{Ty\_Pair\_Elim}$$

$$\frac{\Theta \vdash t' \ \mathsf{Type} \quad \Theta; \Delta; \Gamma, x : t' \vdash e : t}{\Theta; \Delta; \Gamma \vdash \mathbf{fun}\, x : t' \rightarrow e : t' \multimap t} \quad \textsc{Ty\_Lambda}$$

$$\frac{\Theta; \Delta; \Gamma \vdash e : t' \multimap t \quad \Theta; \Delta; \Gamma' \vdash e' : t'}{\Theta; \Delta; \Gamma, \Gamma' \vdash e\, e' : t} \quad \textsc{Ty\_App}$$

$$\frac{\Theta, fc; \Delta; \Gamma \vdash e : t}{\Theta; \Delta; \Gamma \vdash \mathbf{fun}\, fc \rightarrow e : \forall fc.t} \quad \textsc{Ty\_Gen}$$

$$\frac{\Theta \vdash f \ \mathsf{Cap} \quad \Theta; \Delta; \Gamma \vdash e : \forall fc.t}{\Theta; \Delta; \Gamma \vdash e[f] : t[f/fc]} \quad \textsc{Ty\_Spc}$$

$$\frac{\Theta; \Delta, g : t \multimap t'; \cdot, x : t \vdash e : t'}{\Theta; \Delta; \cdot \vdash \mathbf{fix}\,(g, x : t, e : t') : t \multimap t'} \quad \textsc{Ty\_Fix}$$

2 Dynamic Semantics

$\boxed{\langle \sigma, e \rangle \rightarrow \mathit{StepsTo}}$ operational semantics

$$\frac{}{\langle \sigma, \mathbf{let}\,() = ()\,\mathbf{in}\, e \rangle \rightarrow \langle \sigma, e \rangle} \quad \textsc{Op\_Let\_Unit}$$

$$\frac{}{\langle \sigma, \mathbf{let}\, x = v\,\mathbf{in}\, e \rangle \rightarrow \langle \sigma, e[x/v] \rangle} \quad \textsc{Op\_Let\_Var}$$

$$\frac{}{\langle \sigma, \mathbf{if}\,(\mathbf{Many}\,\mathbf{true})\,\mathbf{then}\, e_1\,\mathbf{else}\, e_2 \rangle \rightarrow \langle \sigma, e_1 \rangle} \quad \textsc{Op\_If\_True}$$

$$\frac{}{\langle \sigma, \mathbf{if}\,(\mathbf{Many}\,\mathbf{false})\,\mathbf{then}\, e_1\,\mathbf{else}\, e_2 \rangle \rightarrow \langle \sigma, e_2 \rangle} \quad \textsc{Op\_If\_False}$$

$$\frac{}{\langle \sigma, \mathbf{let}\,\mathbf{Many}\, x = \mathbf{Many}\, v\,\mathbf{in}\, e \rangle \rightarrow \langle \sigma, e[x/v] \rangle} \quad \textsc{Op\_Let\_Many}$$

$$\frac{}{\langle \sigma, \mathbf{let}\,(a, b) = (v_1, v_2)\,\mathbf{in}\, e \rangle \rightarrow \langle \sigma, e[a/v_1][b/v_2] \rangle} \quad \textsc{Op\_Let\_Pair}$$

$$\frac{}{\langle \sigma, (\mathbf{fun}\, fc \rightarrow v)[f] \rangle \rightarrow \langle \sigma, v[fc/f] \rangle} \quad \textsc{Op\_Frac\_Cap}$$

$$\frac{}{\langle \sigma, \mathbf{fix}\,(g, x : t, e : t')\, v \rangle \rightarrow \langle \sigma, e[x/v][g/\mathbf{fix}\,(g, x : t, e : t')] \rangle} \quad \textsc{Op\_App\_Fix}$$

$$\frac{}{\langle \sigma, (\mathbf{fun}\, x : t \rightarrow e)\, v \rangle \rightarrow \langle \sigma, e[x/v] \rangle} \quad \textsc{Op\_App\_Lambda}$$

$$\frac{\langle \sigma, e \rangle \rightarrow \langle \sigma', e' \rangle}{\langle \sigma, C[e] \rangle \rightarrow \langle \sigma, C[e'] \rangle} \quad \textsc{Op\_Context}$$

$$\frac{\langle \sigma, e\rangle \to \mathbf{err}}{\langle \sigma, C[e]\rangle \to \mathbf{err}} \quad \textsc{Op\_Context\_Err}$$

$$\frac{0 \le k_1, k_2 \qquad l \text{ fresh}}{\langle \sigma, \mathbf{matrix}\, k_1\, k_2\rangle \to \langle \sigma + \{l \mapsto_1 M_{k_1,k_2}\}, l\rangle} \quad \textsc{Op\_Matrix}$$

$$\frac{}{\langle \sigma + \{l \mapsto_1 m_{k_1,k_2}\}, \mathbf{free}\, l\rangle \to \langle \sigma, ()\rangle} \quad \textsc{Op\_Free}$$

$$\frac{}{\langle \sigma + \{l \mapsto_f m_{k_1,k_2}\}, \mathbf{share}[f]\, l\rangle \to \langle \sigma + \{l \mapsto_{\frac{1}{2}f} m_{k_1,k_2}\} + \{l \mapsto_{\frac{1}{2}f} m_{k_1,k_2}\}, (l, l)\rangle} \quad \textsc{Op\_Share}$$

$$\frac{f \le 1}{\langle \sigma + \{l \mapsto_{\frac{1}{2}f} m_{k_1,k_2}\} + \{l \mapsto_{\frac{1}{2}f} m_{k_1,k_2}\}, \mathbf{unshare}[f]\, l\, l\rangle \to \langle \sigma + \{l \mapsto_f m_{k_1,k_2}\}, l\rangle} \quad \textsc{Op\_Unshare\_Eq}$$

$$\frac{l \ne l'}{\langle \sigma + \{l \mapsto_{\frac{1}{2}f} m_{k_1,k_2}\} + \{l' \mapsto_{\frac{1}{2}f} m'_{k_1,k_2}\}, \mathbf{unshare}[f]\, l\, l'\rangle \to \mathbf{err}} \quad \textsc{Op\_Unshare\_Neq}$$

$$\frac{\begin{array}{l}\sigma' \equiv \sigma + \{l_1 \mapsto_{fc_1} m_{1\,k_1,k_2}\} + \{l_2 \mapsto_{fc_2} m_{2\,k_2,k_3}\} \\ \sigma_1 \equiv \sigma' + \{l_3 \mapsto_1 m_{3\,k_1,k_3}\} \\ \sigma_2 \equiv \sigma' + \{l_3 \mapsto_1 (m_1\, m_2 + m_3)_{k_1,k_3}\}\end{array}}{\langle \sigma_1, \mathbf{gemm}[fc_1]\, l_1 [fc_2]\, l_2\, l_3\rangle \to \langle \sigma_2, ((l_1, l_2), l_3)\rangle} \quad \textsc{Op\_Gemm\_Match}$$

$$\frac{\begin{array}{l}k_2 \ne k_2' \\ \sigma' \equiv \sigma + \{l_1 \mapsto_{fc_1} m_{1\,k_1,k_2}\} + \{l_2 \mapsto_{fc_2} m_{2\,k_2',k_3}\}\end{array}}{\langle \sigma' + \{l_3 \mapsto_1 m_{1\,k_1,k_3}\}, \mathbf{gemm}[fc_1]\, l_1 [fc_2]\, l_2\, l_3\rangle \to \mathbf{err}} \quad \textsc{Op\_Gemm\_Mismatch}$$

3 Interpretation

3.1 Definitions

Operationally, $\mathit{Heap} \sqsubseteq \mathit{Loc} \times \mathit{Permission} \times \mathit{Matrix}$ (a multiset), denoted with a σ.
Define its *interpretation* to be $\mathit{Loc} \rightharpoonup \mathit{Permission} \times \mathit{Matrix}$ with $\star : \mathit{Heap} \times \mathit{Heap} \rightharpoonup \mathit{Heap}$ as follows:

$$(\varsigma_1 \star \varsigma_2)(l) \equiv \begin{cases} \varsigma_1(l) & \text{if } l \in \mathrm{dom}(\varsigma_1) \wedge l \notin \mathrm{dom}(\varsigma_2) \\ \varsigma_2(l) & \text{if } l \in \mathrm{dom}(\varsigma_2) \wedge l \notin \mathrm{dom}(\varsigma_1) \\ (f_1 + f_2, m) & \text{if } (f_1, m) = \varsigma_1(l) \wedge (f_2, m) = \varsigma_2(l) \wedge f_1 + f_2 \le 1 \\ \text{undefined} & \text{otherwise} \end{cases}$$

Commutativity and associativity of $\star$ follows from that of $+$.
$\varsigma_1 \star \varsigma_2$ is *defined* if it is for all $l \in \mathrm{dom}(\varsigma_1) \cup \mathrm{dom}(\varsigma_2)$.
Implicitly denote $\varsigma \equiv \mathcal{H}[\![\sigma]\!] \equiv \bigstar_{(l,f,m)\in\sigma}[l \mapsto_f m]$.

The $n-$fold iteration for the *StepsTo* (functional) relation, is also a (functional) relation:

$$\forall n.\ \mathbf{err} \to^n \mathbf{err} \qquad \langle \sigma, v\rangle \to^n \langle \sigma, v\rangle \qquad \langle \sigma, e\rangle \to^0 \langle \sigma, e\rangle \qquad \langle \sigma, e\rangle \to^{n+1} ((\langle \sigma, e\rangle \to) \to^n)$$

Hence, all bounded iterations end in either an **err**, a heap-and-expression or a heap-and-value.

3.2 Interpretation

$$\mathcal{V}_k[\![\mathbf{unit}]\!] = \{(\emptyset, *)\}$$

$$\mathcal{V}_k[\![\mathbf{bool}]\!] = \{(\emptyset, true), (\emptyset, false)\}$$

$$\mathcal{V}_k[\![\mathbf{int}]\!] = \{(\emptyset, n) \mid 2^{-63} \leq n \leq 2^{63} - 1\}$$

$$\mathcal{V}_k[\![\mathbf{elt}]\!] = \{(\emptyset, f) \mid f \text{ a IEEE Float64 }\}$$

$$\mathcal{V}_k[\![f\,\mathbf{mat}]\!] = \{(\{l \mapsto_{2^{-f}} \_\}, l)\}$$

$$\mathcal{V}_k[\![!t]\!] = \{(\emptyset, \mathbf{Many}\, v) \mid (\emptyset, v) \in \mathcal{V}_k[\![t]\!]\}$$

$$\mathcal{V}_k[\![\forall fc.\ t]\!] = \{(\varsigma, \mathbf{fun}\, fc \to\ e) \mid \forall f.\ (\varsigma, (\mathbf{fun}\, fc \to\ e)\,[f]) \in \mathcal{C}_k[\![t[fc/f]]\!]\}$$

$$\mathcal{V}_k[\![t_1 \otimes t_2]\!] = \{(\varsigma_1 \star \varsigma_2, (v_1, v_2)) \mid (\varsigma_1, v_1) \in \mathcal{V}_k[\![t_1]\!] \wedge (\varsigma_2, v_2) \in \mathcal{V}_k[\![t_2]\!]\}$$

$$\begin{aligned}\mathcal{V}_k[\![t' \multimap t]\!] = \{(\varsigma_v, v) \mid {} & (v \equiv \mathbf{fun}\, x : t \to e \vee v \equiv \mathbf{fix}(g, x : t', e : t)) \wedge \\ & \forall j \leq k, (\varsigma_{v'}, v') \in \mathcal{V}_j[\![t']\!].\ \varsigma_v \star \varsigma_v' \text{ defined } \Rightarrow (\varsigma_v \star \varsigma_v', v\, v') \in \mathcal{C}_j[\![t]\!]\}\end{aligned}$$

$$\begin{aligned}\mathcal{C}_k[\![t]\!] = \{(\varsigma_s, e_s) \mid {} & \forall\, j < k, \sigma_r.\ \varsigma_s \star \varsigma_r \text{ defined } \Rightarrow \langle \sigma_s + \sigma_r, e_s \rangle \to^j \mathbf{err}\ \vee \exists \sigma_f, e_f. \\ & \langle \sigma_s + \sigma_r, e_s \rangle \to^j \langle \sigma_f + \sigma_r, e_f \rangle \wedge (e_f \text{ is a value } \Rightarrow (\varsigma_f \star \varsigma_r, e_f) \in \mathcal{V}_{k-j}[\![t]\!])\}\end{aligned}$$

$$\mathcal{I}_k[\![\cdot]\!]\theta = \{[]\}$$

$$\mathcal{I}_k[\![\Delta, x : t]\!]\theta = \{\delta[x \mapsto v_x] \mid \delta \in \mathcal{I}_k[\![\Delta]\!]\theta \wedge (\emptyset, v_x) \in \mathcal{V}_k[\![\theta(t)]\!]\}$$

$$\mathcal{L}_k[\![\cdot]\!]\theta = \{(\emptyset, [])\}$$

$$\mathcal{L}_k[\![\Gamma, x : t]\!]\theta = \{(\varsigma \star \varsigma_x, \gamma[x \mapsto v_x]) \mid (\varsigma, \gamma) \in \mathcal{L}_k[\![\Gamma]\!]\theta \wedge (\varsigma_x, v_x) \in \mathcal{V}_k[\![\theta(t)]\!]\}$$

$$\varsigma \equiv \mathcal{H}[\![\sigma]\!] \equiv \bigstar_{(l,f,m) \in \sigma}[l \mapsto_f m]$$

$$\begin{aligned}{}_k[\![\Theta; \Delta; \Gamma \vdash e : t]\!] = {} & \forall \theta, \delta, \gamma, \sigma.\ \Theta = \mathrm{dom}(\theta) \wedge (\varsigma, \gamma) \in \mathcal{L}_k[\![\Gamma]\!]\theta \wedge \delta \in \mathcal{I}_k[\![\Delta]\!]\theta \Rightarrow \\ & (\varsigma, \theta(\gamma(\delta(e)))) \in \mathcal{C}_k[\![\theta(t)]\!]\end{aligned}$$

4 Proofs

4.1 Lemmas

4.1.1 $\forall \sigma_s, \sigma_r, e.\ \varsigma_s \star \varsigma_r$ **defined** $\Rightarrow \forall n.\ \langle \sigma_s, e\rangle \to^n = \langle \sigma_s + \sigma_r, e\rangle \to^n$

Suffices: By induction on n, consider only the cases $\langle \sigma_s, e\rangle \to \langle \sigma_f, e_f\rangle$ where $\sigma_s \neq \sigma_f$.

Proof sketch: Only Op_{Free, Matrix, Share, Unshare_Eq, Gemm_Match} change the heap: the rest are either parametric in the heap or step to an **err**.

Prove: $\langle \sigma_s + \sigma_r, e\rangle \to \langle \sigma_f + \sigma_r, e_f\rangle$.

$\langle 1\rangle 1$. Case: Op_Free, $\sigma_s \equiv \sigma' + \{l \mapsto_1 m\}$, $\sigma_f = \sigma'$.
Proof: Instantiate Op_Free with $(\sigma' + \sigma_r) + \{l \mapsto_1 m\}$,
valid because $l \notin \mathrm{dom}(\varsigma_r)$ by $\varsigma' \star [l \mapsto_1 m] \star \varsigma_r$ defined (assumption).

$\langle 1\rangle 2$. Case: Op_Matrix
Proof: Rule has no requirements on σ_s so will also work with $\sigma_s + \sigma_r$.

$\langle 1\rangle 3$. Case: Op_Share, $\sigma_s \equiv \sigma' + \{l \mapsto_f m\}$, $\sigma_f = \sigma' + \{l \mapsto_{\frac{1}{2}\cdot f} m\} + \{l \mapsto_{\frac{1}{2}\cdot f} m\}$.
Proof: Union-ing σ_r does not remove $l \mapsto_f m$, so that can be split out of $\sigma_s + \sigma_r$ as before.

$\langle 1\rangle 4$. Case: Op_Unshare_Eq, $\sigma_s \equiv \sigma' + \{l \mapsto_{\frac{1}{2}\cdot f} m\} + \{l \mapsto_{\frac{1}{2}\cdot f} m\}$, $\sigma_f = \sigma' + \{l \mapsto_f m\}$.

- $\langle 2\rangle 1$. Union-ing σ_r does not remove $l \mapsto_{\frac{1}{2}\cdot f} m$, so that can still be split out of $\sigma_s + \sigma_r$.
- $\langle 2\rangle 2$. There may also be other valid splits introduced by σ_r.
- $\langle 2\rangle 3$. However, by assumption of $\varsigma_s \star \varsigma_r$ defined, any splitting of $\sigma_s + \sigma_r$ will satisfy $f \leq 1$.

$\langle 1\rangle 5$. Case: Op_Gemm_Match

- $\langle 2\rangle 1$. By assumption of $\varsigma_s \star \varsigma_r$ defined, either l_1 (or l_2, or both) are not in σ_r, or they are and the matrix values they point to are the same.
- $\langle 2\rangle 2$. The permissions (of l_1 and/or l_2) may differ, but Op_Gemm_Match universally quantifies over them and leaves them unchanged, so they are irrelevant.
- $\langle 2\rangle 3$. Only the pointed to matrix value at l_3 changes.
- $\langle 2\rangle 4$. Suffices: $l_3 \notin \pi_1[\sigma_r]$.
- $\langle 2\rangle 5$. By assumption of $\varsigma_s \star \varsigma_r$ defined, $l_3 \notin \mathrm{dom}(\varsigma_r)$.
- $\langle 2\rangle 6$. Hence $l_3 \notin \pi_1[\sigma_r]$.

4.1.2 $\forall k, t.\ \mathcal{V}_k[\![t]\!] \subseteq \mathcal{C}_k[\![t]\!]$

Follows from definition of $\mathcal{C}_k[\![t]\!]$, $\to^j$ $(\forall n.\ \langle \sigma, v\rangle \to^n \langle \sigma, v\rangle)$ for arbitrary $j \leq k$ and 4.1.1.

4.1.3 $\forall \theta, \delta, \gamma, v.\ \theta(\delta(\gamma(v)))$ is a value.

θ is irrelevant because it only maps fractional capability variables to fractional capabilities. By construction, δ and γ only map variables to values, and values are closed under substitution.

4.1.4 $\forall k, \sigma, \sigma', e, e', t.\ (\varsigma', e') \in \mathcal{C}_k[\![t]\!] \wedge \langle \sigma, e\rangle \rightarrow \langle \sigma', e'\rangle \Rightarrow (\varsigma, e) \in \mathcal{C}_{k+1}[\![t]\!]$

ASSUME: arbitrary $j < k+1$, and σ_r such that $\varsigma \star \varsigma_r$ defined.

$\langle 1\rangle 1.$ CASE: $j = 0$. Clearly $\sigma_f = \sigma_s + \sigma_r$ and $e' = e$.
Remains to show that if e is a value then $(\varsigma_s \star \varsigma_r, e) \in \mathcal{V}_k[\![t]\!]$.
This is true vacuously, because by assumption, e is not a value.

$\langle 1\rangle 2.$ CASE: $j \geq 1$. We have $\langle \sigma, e\rangle \rightarrow^j = \langle \sigma', e'\rangle \rightarrow^{j-1}$.
Instantiate $(\varsigma', e') \in \mathcal{C}_k[\![t]\!]$, with $j-1 < k$ and σ_r to conclude the required conditions.

4.1.5 $j \leq k \Rightarrow {}_{-\,k}[\![\cdot]\!] \subseteq {}_{-\,j}[\![\cdot]\!]$

Lemma 4.1.4 is the inductive step for this lemma for the $\mathcal{C}[\![]\!]$ case.
Need to prove for $\mathcal{V}[\![]\!]$, by induction on t and then index.

SUFFICES: Consider only $t \multimap t'$ case, rest use k directly on structure of type.
ASSUME: Arbitrary $j \leq k$ and $(\varsigma_{v'}, v') \in \mathcal{V}_k[\![t \multimap t']\!]$.
PROVE: $(\varsigma_{v'}, v') \in \mathcal{V}_j[\![t \multimap t']\!]$.

$\langle 1\rangle 1.$ v' is of the correct syntactic form (lambda or fixpoint) by assumption.

$\langle 1\rangle 2.$ ASSUME: arbitrary $j' \leq j$ and $(\varsigma_v, v) \in \mathcal{V}_{j'}[\![t]\!]$ such that $\varsigma_{v'} \star \varsigma_v$ is defined.

$\langle 1\rangle 3.$ SUFFICES: to show $(\varsigma_{v'} \star \varsigma_v, v'v) \in \mathcal{C}_{j'}[\![t']\!]$.

$\langle 1\rangle 4.$ This is true by instantiating $(\varsigma_{v'}, v') \in \mathcal{V}_k[\![t \multimap t']\!]$ with $j' \leq k$ and $(\varsigma_v, v) \in \mathcal{V}_{j'}[\![t]\!]$.

4.1.6 $\forall \Delta, \Gamma, t, k, \theta, \delta, \gamma.\ \delta \in \mathcal{I}_k[\![\Delta]\!]\theta \wedge \gamma \in \pi_2[\mathcal{L}_k[\![\Gamma]\!]\theta] \Rightarrow \mathrm{dom}(\Delta) = \mathrm{dom}(\delta)$ and $\mathrm{dom}(\Gamma) = \mathrm{dom}(\gamma)$

PROOF: By induction on Δ and Γ.

4.1.7 $\forall k, \Gamma, \Gamma', \theta, \sigma_+, \gamma_+.\ (\varsigma_+, \gamma) \in \mathcal{L}_k[\![\Gamma, \Gamma']\!]\theta \wedge \Gamma, \Gamma'$ disjoint $\Rightarrow$ $\exists \sigma, \gamma, \sigma', \gamma'.\ \sigma_+ = \sigma + \sigma' \wedge \gamma, \gamma'$ disjoint $\wedge\, \gamma_+ = \gamma \cup \gamma'$ $\wedge\, (\varsigma, \gamma) \in \mathcal{L}_k[\![\Gamma]\!] \wedge (\varsigma', \gamma') \in \mathcal{L}_k[\![\Gamma']\!]$

PROOF: By induction on Γ'.

4.2 Soundness

$$\forall \Theta, \Delta, \Gamma, e, t.\ \Theta; \Delta; \Gamma \vdash e : t \Rightarrow \forall k.\ {}_k[\![\Theta; \Delta; \Gamma \vdash e : t]\!]$$

PROOF SKETCH: Induction over the typing judgements.

ASSUME: 1. Arbitrary $\Theta, \Delta, \Gamma, e, t$ such that $\Theta; \Delta; \Gamma \vdash e : t$.
2. Arbitrary $k, \theta, \delta, \gamma, \sigma$ such that:
a. $\Theta = \mathrm{dom}(\theta)$
b. $(\varsigma, \gamma) \in \mathcal{L}_k[\![\Gamma]\!]\theta$
c. $\delta \in \mathcal{I}_k[\![\Delta]\!]\theta$.
3. W.l.o.g., all variables are distinct, hence Θ, $\mathrm{dom}(\Delta)$ and $\mathrm{dom}(\Gamma)$ are disjoint so order of θ, δ and γ (as substitutions defined recursively over expressions) is irrelevant.

PROVE: $(\varsigma, \theta(\gamma(\delta(e)))) \in \mathcal{C}_k[\![\theta(t)]\!]$.
ASSUME: Arbitrary $j < k$ and σ_r, such that $\varsigma \star \varsigma_r$ defined.
SUFFICES: $\langle \sigma + \sigma_r, e \rangle \to^j \mathbf{err}\ \vee \exists \sigma_f, e_f.\ \langle \sigma + \sigma_r, e \rangle \to^j \langle \sigma_f + \sigma_r, e_f \rangle$
$\wedge$ (e_f is a value $\Rightarrow (\varsigma_f \star \varsigma_r, e_f) \in \mathcal{V}_{k-j}[\![t]\!]$).
SUFFICES: By 4.1.1, to show $\langle \sigma, e \rangle \to^j \mathbf{err}\ \vee \exists \sigma_f, e_f.\ \langle \sigma, e \rangle \to^j \langle \sigma_f, e_f \rangle$
$\wedge$ (e_f is a value $\Rightarrow (\varsigma_f, e_f) \in \mathcal{V}_{k-j}[\![t]\!]$)

⟨1⟩1. CASE: TY_LET.

⟨2⟩1. By induction,
1. $\forall k.\ {}_k[\![\Theta; \Delta; \Gamma \vdash e : t]\!]$
2. $\forall k.\ {}_k[\![\Theta; \Delta; \Gamma', x : t \vdash e' : t']\!]$.

⟨2⟩2. By 2b, 3 and 4.1.7, we know there exists the following (for all k):
1. $(\varsigma_e, \gamma_e) \in \mathcal{L}_k[\![\Gamma]\!]$
2. $\gamma = \gamma_e \cup \gamma_{e'}$
3. $\sigma = \sigma_e + \sigma_{e'}$.

⟨2⟩3. So, using $k, \theta, \delta, \gamma_e, \sigma_e$, we have $(\varsigma_e, \theta(\gamma_e(\delta(e)))) \in \mathcal{C}_k[\![\theta(t)]\!]$.

⟨2⟩4. By ⟨2⟩2 ($\gamma = \gamma_e \cup \gamma_{e'}$), have $(\varsigma_e, \theta(\gamma(\delta(e)))) \in \mathcal{C}_k[\![\theta(t)]\!]$.

⟨2⟩5. By definition of $\mathcal{C}_k[\![\cdot]\!]$ and ⟨2⟩2, we instantiate with j and $\sigma_r = \sigma_{e'}$ to conclude that $\langle \varsigma, \theta(\gamma(\delta(e))) \rangle$ either takes j steps to **err** or another heap-and-expression $\langle \sigma_f, \theta(\gamma(\delta(e_f))) \rangle$.

⟨2⟩6. CASE: j steps to **err**
By OP_CONTEXT_ERR, the whole expression reduces to **err** in $j < k$ steps.

⟨2⟩7. CASE: j steps to another heap-and-expression.
If it is not a value, then OP_CONTEXT runs j times and we are done.

⟨2⟩8. If it is, then $\exists i \le j.\ (\varsigma_f, v_1) \in \mathcal{V}_{k-i}[\![\theta(t_1)]\!] \subseteq \mathcal{V}_{k-j}[\![\theta(t_1)]\!]$ by 4.1.3 and 4.1.5.
So, OP_CONTEXT runs i times, and then we have the following.
SUFFICES: $(\varsigma_f \star \varsigma_{e'}, \mathbf{let}\, x = v\, \mathbf{in}\, \theta(\gamma(\delta(e')))) \in \mathcal{C}_{k-i}[\![\theta(t')]\!]$ by 4.1.4 i times.
SUFFICES: $(\varsigma_f \star \varsigma_{e'}, \theta(\gamma(\delta(e')))[x/v]) \in \mathcal{C}_{k-i-1}[\![\theta(t')]\!]$ by 4.1.4.

⟨2⟩9. By 4.1.5, $(\varsigma_{e'}, \gamma_{e'}[x \mapsto v]) \in \mathcal{L}_k[\![\Gamma', x : t]\!]\theta \subseteq \mathcal{L}_{k-i-1}[\![\Gamma', x : t]\!]\theta$.

⟨2⟩10. Instantiate 2 of step ⟨2⟩1 with $k - i - 1, \theta, \delta, \gamma_{e'}[x \mapsto v], \sigma_{e'}$ to conclude $(\varsigma_{e'}, \theta(\gamma_{e'}[x \mapsto v](\delta(e')))) \in \mathcal{C}_{k-i-1}[\![\theta(t')]\!]$.

⟨2⟩11. By 3, we have $\theta(\gamma(\delta(e')))[x/v] = \theta(\gamma_{e'}[x \mapsto v](\delta(e')))$ and by 4.1.1 we conclude $(\varsigma_f \star \varsigma_{e'}, \theta(\gamma(\delta(e')))[x/v]) \in \mathcal{C}_{k-i-1}[\![\theta(t')]\!]$

⟨1⟩2. CASE: TY_PAIR_ELIM.
PROOF SKETCH: Similar to TY_LET, but with the following key differences.

⟨2⟩1. When $(\varsigma_f, v) \in \mathcal{V}_{k-i}[\![\theta(t_1) \otimes \theta(t_2)]\!]$, we have $v = (v_1, v_2)$.

⟨2⟩2. SUFFICES: $(\varsigma_{e'}, \theta(\gamma(\delta(e')))) \in \mathcal{C}_{k-i-1}[\![\theta(t')]\!]$ by 4.1.4 $i+1$ times.

⟨2⟩3. By 4.1.5, $(\varsigma_{e'}, \gamma_{e'}[a \mapsto v_1, b \mapsto v_2]) \in \mathcal{L}_k[\![\Gamma', a : t_1, b : t_2]\!]\theta \subseteq \mathcal{L}_{k-i-1}[\![\Gamma', a : t_1, b : t_2]\!]\theta$.

⟨2⟩4. Instantiate $_{k-i-1}[\![\Theta; \Delta; \Gamma', a : t_1, b : t_2 \vdash e' : t']\!]$ with $\theta, \delta, \gamma_{e'}[a \mapsto v_1, b \mapsto v_2], \sigma_{e'}$.

⟨2⟩5. By 3 (for $\gamma = \gamma_e \cup \gamma_{e'}$ and a, b), conclude $(\varsigma_{e'}, \theta(\gamma(\delta(e'[a/v_1][b/v_2])))) \in \mathcal{C}_{k-i-1}[\![\theta(t')]\!]$.

⟨1⟩3. CASE: TY_BANG_ELIM.
PROOF SKETCH: Similar to TY_LET, but with the following key differences.

⟨2⟩1. When $(\varsigma_f, v) \in \mathcal{V}_{k-i}[\![\theta(!t)]\!]$, since $\mathcal{V}_{k-i}[\![\theta(!t)]\!] = \mathcal{V}_{k-i}[\![!\theta(t)]\!]$, we have $\varsigma_f = \emptyset$ and $v = \textbf{Many}\, v'$ for some $(\emptyset, v') \in \mathcal{V}_{k-i}[\![\theta(t)]\!]$.

⟨2⟩2. SUFFICES: $(\varsigma_{e'}, \textbf{let Many}\, x \ = \ \textbf{Many}\, v' \,\textbf{in}\, \theta(\gamma(\delta(e')))) \in \mathcal{C}_{k-i}[\![\theta(t)]\!]$.

⟨2⟩3. SUFFICES: $(\varsigma_{e'}, \theta(\gamma(\delta(e')))[x/v]) \in \mathcal{C}_{k-i-1}[\![\theta(t)]\!]$ by 4.1.4 $i+1$ times.

⟨2⟩4. Instantiate $_{k-i-1}[\![\Theta; \Delta, x : t, \Gamma' \vdash e' : t']\!]$ with $\theta, \delta_{e'} = \delta[x \mapsto v'], \gamma_{e'}, \sigma_{e'}$.

⟨2⟩5. By 3, $(\varsigma_{e'}, \theta(\gamma(\delta(e')))[x/v]) \in \mathcal{C}_{k-i-1}[\![\theta(t)]\!]$.

⟨1⟩4. CASE: TY_UNIT_ELIM.
PROOF SKETCH: Similar to TY_LET, but with the following key differences.

⟨2⟩1. When $(\varsigma_f, v) \in \mathcal{V}_{k-i}[\![\textbf{unit}]\!]$, we have $\varsigma_f = \emptyset$ and $v = ()$.

⟨2⟩2. SUFFICES: $(\varsigma_{e'}, \theta(\gamma(\delta(e')))) \in \mathcal{C}_{k-i-1}[\![\theta(t')]\!]$ by 4.1.4 $i+1$ times.

⟨2⟩3. By 4.1.5, $(\varsigma_{e'}, \gamma_{e'}) \in \mathcal{L}_k[\![\Gamma']\!]\theta \subseteq \mathcal{L}_{k-i-1}[\![\Gamma']\!]\theta$.

⟨2⟩4. Instantiate $_{k-i-1}[\![\Theta; \Delta; \Gamma' \vdash e' : t']\!]$ with $\theta, \delta, \gamma_{e'}, \sigma_{e'}$.

⟨2⟩5. By 3 $(\varsigma_{e'}, \theta(\gamma(\delta(e')))) \in \mathcal{C}_{k-i-1}[\![\theta(t')]\!]$.

⟨1⟩5. CASE: TY_BOOL_ELIM.
PROOF SKETCH: Similar to TY_UNIT_ELIM but with OP_IF_{TRUE,FALSE}, $\varsigma_f = \emptyset$ and $v = \textbf{Many true}$ or $v = \textbf{Many false}$.

⟨1⟩6. CASE: TY_BANG_INTRO.

⟨2⟩1. We have, $e = v$ for some value $v \neq l \cdot f$, $\Gamma = \emptyset$ and so $\forall k.\ _k[\![\Theta; \Delta; \cdot \vdash v : t]\!]$ by induction.

⟨2⟩2. SUFFICES: $(\emptyset, \textbf{Many}\, \delta(v)) \in \mathcal{C}_k[\![!\theta(t)]\!]$ by 2b $(\varsigma = \emptyset, \gamma = [])$.

⟨2⟩3. Instantiate $_k[\![\Theta; \Delta; \cdot \vdash v : t]\!]$ with $\theta, \delta, \gamma = [], \sigma = \emptyset$ to obtain $(\emptyset, \delta(v)) \in \mathcal{C}_k[\![\theta(t)]\!]$.

⟨2⟩4. Instantiate $(\emptyset, \delta(v)) \in \mathcal{C}_k[\![\theta(t)]\!]$ with $j = 0$, $\sigma_r = \emptyset$ and 4.1.3 ($\delta(v)$ is a value), to conclude $(\emptyset, \delta(v)) \in \mathcal{V}_k[\![\theta(t)]\!]$.

$\langle 2\rangle 5.$ By definition of $\mathcal{V}_k[\![!\theta(t)]\!]$, 4.1.3 and 4.1.2 we have $(\emptyset, \mathbf{Many}\,\delta(v)) \in \mathcal{C}_k[\![!\theta(t)]\!]$.

$\langle 1\rangle 7.$ CASE: TY_PAIR_INTRO.

$\langle 2\rangle 1.$ By 2b, 3 and 4.1.7, we know there exists the following (for all k):
1. $(\varsigma_1, \gamma_1) \in \mathcal{L}_k[\![\Gamma_1]\!]$
2. $(\varsigma_2, \gamma_2) \in \mathcal{L}_k[\![\Gamma_2]\!]$
3. $\gamma = \gamma_1 \cup \gamma_2$
4. $\sigma = \sigma_1 + \sigma_2$.

$\langle 2\rangle 2.$ By induction,
1. $\forall k.\ {}_k[\![\Theta; \Delta; \Gamma_1 \vdash e_1 : t_1]\!]$
2. $\forall k.\ {}_k[\![\Theta; \Delta; \Gamma_2 \vdash e_2 : t_2]\!]$.

$\langle 2\rangle 3.$ Instantiate the first with $k, \theta, \delta, \gamma_1, \sigma_1$.

$\langle 2\rangle 4.$ By that and $\langle 2\rangle 1$, $(\varsigma_1, \theta(\gamma_1(\delta(e_1)))) = (\varsigma_1, \theta(\gamma(\delta(e_1)))) \in \mathcal{C}_k[\![\theta(t)]\!]$.

$\langle 2\rangle 5.$ So, $\langle \sigma_1 + \sigma_2, \theta(\gamma_1(\delta(e_1)))\rangle$ either takes j steps to **err** or a heap-and-expression $\langle \sigma_{1f}, e_{1f}\rangle$.

$\langle 2\rangle 6.$ CASE: j steps to **err**
By OP_CONTEXT_ERR, the whole expression reduces to **err** in $j < k$ steps.

$\langle 2\rangle 7.$ CASE: j steps to another heap-and-expression.
If it is not a value, then OP_CONTEXT runs j times and we are done.

$\langle 2\rangle 8.$ If it is, then $\exists i_1 \leq j.\ (\varsigma_{1f}, v_1) \in \mathcal{V}_{k-i_1}[\![\theta(t_1)]\!] \subseteq \mathcal{V}_{k-j}[\![\theta(t_1)]\!]$ by 4.1.3 and 4.1.5.
So, OP_CONTEXT runs i_1 times, and then we have the following.
SUFFICES: By 4.1.4, $(\varsigma_{1f} \star \varsigma_2,\ (v_1, e_2)\,) \in \mathcal{C}_{k-i_1}[\![\theta(t_1 \otimes t_2)]\!]$.

$\langle 2\rangle 9.$ Instantiate the second IH with $k, \theta, \delta, \gamma_2, \sigma_2$.

$\langle 2\rangle 10.$ So, $\langle \sigma_{1f} \star \sigma_2, \theta(\gamma_2(\delta(e_2)))\rangle$ either takes j steps to **err** or a heap-and-expression $\langle \sigma_{2f}, e_{2f}\rangle$.

$\langle 2\rangle 11.$ CASE: j steps to **err**
By OP_CONTEXT_ERR, the whole expression reduces to **err** in $j < k$ steps.

$\langle 2\rangle 12.$ CASE: j steps to another heap-and-expression.
If it is not a value, then OP_CONTEXT runs j times and we are done.

$\langle 2\rangle 13.$ If it is, then $\exists i_2 \leq j.\ (\varsigma_{2f}, v_2) \in \mathcal{V}_{k-i_2}[\![\theta(t_2)]\!] \subseteq \mathcal{V}_{k-j}[\![\theta(t_2)]\!]$ by 4.1.3 and 4.1.5.
So, OP_CONTEXT runs i_2 times, and then we have the following.
SUFFICES: By 4.1.4, $(\varsigma_{1f} \star \varsigma_{2f},\ (v_1, v_2)\,) \in \mathcal{V}_{k-i_1-i_2}[\![\theta(t_1) \otimes \theta(t_2)]\!]$.

$\langle 2\rangle 14.$ By 4.1.5 and $k - i_1 - i_2 \leq k - i_1, k - i_2$, have
$(\varsigma_{1f}, v_1) \in \mathcal{V}_{k-i_1}[\![\theta(t_1)]\!] \subseteq \mathcal{V}_{k-i_1-i_2}[\![\theta(t_1)]\!]$ and
$(\varsigma_{2f}, v_2) \in \mathcal{V}_{k-i_2}[\![\theta(t_2)]\!] \subseteq \mathcal{V}_{k-i_1-i_2}[\![\theta(t_2)]\!]$ as needed.

$\langle 1\rangle 8.$ CASE: TY_LAMBDA.
SUFFICES: By 4.1.2, to show $(\,\varsigma, \gamma(\delta(\mathbf{fun}\,x : t \to e))\,) \in \mathcal{V}_k[\![\theta(t \multimap t')]\!]$.
ASSUME: Arbitrary $j \leq k$, $(\varsigma_v, v) \in \mathcal{V}_j[\![\theta(t)]\!]$ such that $\varsigma \star \varsigma_v$ is defined.
SUFFICES: $(\varsigma \star \varsigma_v, \gamma(\delta(\mathbf{fun}\,x : t \to e))\,v) \in \mathcal{C}_j[\![\theta(t')]\!]$.
SUFFICES: $(\varsigma \star \varsigma_v, \theta(\gamma(\delta(e)))[x/v]) \in \mathcal{C}_{j-1}[\![\theta(t')]\!]$ by 4.1.4.

⟨2⟩1. By induction, $\forall k.\ {}_k[\![\Theta; \Delta; \Gamma, x : t \vdash e]\!]$.

⟨2⟩2. Instantiate it $j-1, \theta, \gamma[x \mapsto v], \sigma + \sigma_v$.

⟨2⟩3. Hence, $(\,\varsigma \star \varsigma_v, \theta(\gamma[x \mapsto v](\delta(e)))\,) \in \mathcal{C}_{j-1}[\![\theta(t)]\!]$.

⟨2⟩4. By 3, $\theta(\gamma[x \mapsto v](\delta(e))) = \theta(\gamma(\delta(e)))[x/v]$, we are done.

⟨1⟩9. Case: Ty_App.

⟨2⟩1. By 2b, 3 and 4.1.7, we know there exists the following (for all k):
1. $(\varsigma_e, \gamma_e) \in \mathcal{L}_k[\![\Gamma_e]\!]$
2. $(\varsigma_{e'}, \gamma_{e'}) \in \mathcal{L}_k[\![\Gamma_{e'}]\!]$
3. $\gamma = \gamma_e \cup \gamma_{e'}$
4. $\sigma = \sigma_e + \sigma_{e'}$.

⟨2⟩2. By induction,
1. $\forall k.\ {}_k[\![\Theta; \Delta; \Gamma \vdash e : t' \multimap t]\!]$
2. $\forall k.\ {}_k[\![\Theta; \Delta; \Gamma' \vdash e' : t']\!]$.

⟨2⟩3. Instantiate the first with $\theta, k, \delta, \gamma_e, \sigma_e$ to conclude $(\varsigma_e, \theta(\gamma_e(\delta(e)))) \in \mathcal{C}_k[\![\theta(t') \multimap \theta(t)]\!]$.

⟨2⟩4. Instantiate *this* with j and $\sigma_{e'}$ and use ⟨2⟩1 to conclude $\langle \sigma_e + \sigma_{e'}, \theta(\gamma(\delta(e))) \rangle$ either takes j steps to **err** or a heap-and-expression $\langle \sigma_f + \sigma_{e'}, e_f \rangle$.

⟨2⟩5. Case: j steps to **err**
By Op_Context_Err, the whole expression reduces to **err** in $j < k$ steps.

⟨2⟩6. Case: j steps to another heap-and-expression.
If it is not a value, then Op_Context runs j times and we are done.

⟨2⟩7. If it is, then $\exists i_e \leq j.\ (\varsigma_f, v_e) \in \mathcal{V}_{k-i_e}[\![\theta(t') \multimap \theta(t)]\!] \subseteq \mathcal{V}_{k-j}[\![\ldots]\!]$ by 4.1.3 and 4.1.5.
So, Op_Context runs i_e times, and then we have the following.
Suffices: By 4.1.4 i_e times, $(\varsigma_f \star \varsigma_{e'},\ v_e\, e'\,) \in \mathcal{C}_{k-i_e}[\![\theta(t')]\!]$.

⟨2⟩8. By 4.1.5, $(\varsigma_{e'}, \gamma_{e'} \in \mathcal{L}_k[\![\Gamma']\!]\theta \subseteq \mathcal{L}_{k-i_e}[\![\Gamma']\!]\theta$.

⟨2⟩9. So, instantiate the second IH with $k - i_e, \theta, \delta, \gamma_{e'}, \sigma_{e'}$ to conclude $(\varsigma_{e'}, \theta(\gamma_{e'}(\delta(e')))) \in \mathcal{C}_{k-i_e}[\![\theta(t')]\!]$.

⟨2⟩10. Instantiate *this* with $j - i_e$ and σ_f to conclude $\langle \sigma_f + \sigma_{e'}, \theta(\gamma_{e'}(\delta(e'))) \rangle$ either takes $j - i_e$ steps to **err** or $\langle \sigma_f + \sigma_{f'}, e_{f'} \rangle$.

⟨2⟩11. Case: $j - i_e$ steps to **err**
By Op_Context_Err, the whole expression reduces to **err** in $j - i_e < k - i_e$ steps.

⟨2⟩12. Case: $j - i_e$ steps to another heap-and-expression.
If it is not a value, then Op_Context runs $j - i_e$ times and we are done.

⟨2⟩13. If it is, then $\exists i_{e'} \leq j - i_e.\ (\varsigma_{f'}, v_{e'}) \in \mathcal{V}_{k-i_e-i'_e}[\![\theta(t')]\!]$ by 4.1.3.
So, Op_Context runs $i_{e'}$ times, and then we have the following.
Suffices: By 4.1.4 $i_{e'}$ times, $(\varsigma_f \star \varsigma_{f'},\ v_e\, v'_e\,) \in \mathcal{C}_{k-i_e-i_{e'}}[\![\theta(t')]\!]$.

⟨2⟩14. Instantiate $(\varsigma_f, v_e) \in \mathcal{V}_{k-i_e}[\![\theta(t') \multimap \theta(t)]\!]$ with $k - i_e - i_{e'} \leq k - i_e$ and $(\varsigma_{v'}, v_{e'}) \in \mathcal{V}_{k-i_e-i_{e'}}[\![\theta(t')]\!]$, to conclude $(\varsigma_f \star \varsigma_{f'}, v\, v') \in \mathcal{C}_{k-i_e-i_{e'}}[\![\theta(t)]\!]$ as needed.

⟨1⟩10. CASE: TY_GEN.
SUFFICES: By 4.1.2 to show $(\sigma, \theta(\gamma(\delta(\mathbf{fun}\, fc \to e)))) \in \mathcal{V}_k[\![\theta(\forall\, fc.\, t)]\!]$.
ASSUME: Assume arbitrary fraction f.
SUFFICES: $(\varsigma, \theta(\gamma(\delta(\mathbf{fun} fc \to e)))\, [f]) \in \mathcal{C}_k[\![\theta(t)[fc/f]]\!]$.

⟨2⟩1. By induction, $\forall k.\ {}_k[\![\Theta, fc; \Delta; \Gamma \vdash e : t]\!]$.

⟨2⟩2. So using $k, \theta[fc \mapsto f], \gamma, \sigma$ we conclude $(\varsigma, \theta(\gamma(\delta(e)))) \in \mathcal{C}_k[\![\theta(t)[fc/f]]\!]$.

⟨1⟩11. CASE: TY_SPC.
PROVE: $(\sigma, \theta(\gamma(\delta(e\,[f])))) \in \mathcal{C}_k[\![\theta(t\,[fc/f])]\!]$.

⟨1⟩12. CASE: TY_FIX.
PROVE: $(\sigma, \theta(\gamma(\delta(\mathbf{fix}(g, x : t, e : t'))))) \in \mathcal{C}_k[\![\theta(!(t \multimap t'))]\!]$.
SUFFICES: to show $\ldots \in \mathcal{V}_k[\![!(\theta(t) \multimap \theta(t'))]\!]$, by 4.1.2.

⟨2⟩1. ASSUME: Arbitrary $j < k$ and $(\sigma, v) \in \mathcal{V}_j[\![\theta(t)]\!]$.

⟨2⟩2. SUFFICES: $(\sigma, \mathit{letManyG}\ g\, v) \in \mathcal{C}_j[\![\theta(t')]\!]$.

⟨2⟩3. LET: $e_1 = e[g/\mathbf{fun}\, x : t \to \mathit{letManyG}\ g\, x]$.

⟨2⟩4. SUFFICES: by 4.1.4, $(\sigma, (\mathbf{fun}\, x : t \to e_1)\, v) \in \mathcal{C}_{j-1}[\![\theta(t')]\!]$.

⟨2⟩5. SUFFICES: by 4.1.4, $(\sigma, e_1[x/v]) \in \mathcal{C}_{j-2}[\![\theta(t')]\!]$.

⟨2⟩6. By induction, we have $[\![\Theta; \Delta, g : t \multimap t'; x : t \vdash e : t']\!]$.

⟨2⟩7. Instantiate this with $\theta, j-2, \delta[g \mapsto \mathbf{fun}\, x : t \to e_1], \gamma = [x \mapsto v], \sigma$ (???).
PROVE: $(\sigma, \mathbf{fun}\, x : t \to e_1) \in \mathcal{V}_{j-2}[\![\theta(t) \multimap \theta(t')]\!]$.

⟨3⟩1. SUFFICES: by 4.1.4, $(\sigma', e_1[x/v']) \in \mathcal{C}_{j-2}[\![\theta(t')]\!]$ for arbitrary $(\sigma', v') \in \mathcal{V}_{j-2}[\![\theta(t)]\!]$.

⟨3⟩2. We can again use the induction hypothesis $[\![\Theta; \Delta, g : t \multimap t'; x : t \vdash e : t']\!]$.

⟨3⟩3. But since it's true for $\mathcal{C}_0[\![\cdot]\!]$ (base case), it's true by induction ???

⟨2⟩8. Lastly, we show $\delta(\theta(\gamma(e))) = e_1[x/v]$, which follows by their definitions, to conclude $(\sigma, e_1[x/v]) \in \mathcal{C}_{j-2}[\![\theta(t')]\!]$.

⟨1⟩13. CASE: TY_VAR_LIN.
PROVE: $(\sigma, \theta(\gamma(\delta(x)))) \in \mathcal{C}_k[\![\theta(t)]\!]$.

⟨2⟩1. $\Gamma = \{x : t\}$ by assumption of TY_VAR_LIN.

⟨2⟩2. SUFFICES: $(\sigma, \gamma(x)) \in \mathcal{C}_k[\![\theta(t)]\!]$ by 3.

⟨2⟩3. By 2b, there exist $(\sigma_x, v_x) \in \mathcal{V}_k[\![\theta(t)]\!]$, such that $\sigma = \sigma_x$ and $\gamma = [x \mapsto v_x]$.

⟨2⟩4. Hence, $(\sigma_x, v_x) \in \mathcal{C}_k[\![\theta(t)]\!]$, by 4.1.2.

⟨1⟩14. CASE: TY_VAR.
PROVE: $(\sigma, \theta(\gamma(\delta(x)))) \in \mathcal{C}_k[\![\theta(t)]\!]$.

⟨2⟩1. $x : t \in \Delta$ and $\Gamma = \emptyset$ by assumption of TY_VAR.

$\langle 2 \rangle 2$. SUFFICES: $(\emptyset, \delta(x)) \in \mathcal{C}_k[\![\theta(t)]\!]$ by 3 and 2b.

$\langle 2 \rangle 3$. By 2c, there exists v_x such that $(\emptyset, v_x) \in \mathcal{V}_k[\![\theta(t)]\!]$.

$\langle 2 \rangle 4$. Hence, $(\emptyset, v_x) \in \mathcal{C}_k[\![\theta(t)]\!]$, by 4.1.2.

$\langle 1 \rangle 15$. CASE: TY_UNIT_INTRO.
PROVE: $(\sigma, \theta(\gamma(\delta(\,()\,)))) \in \mathcal{C}_k[\![\theta(\mathbf{unit})]\!]$.

$\langle 1 \rangle 16$. CASE: TY_BOOL_TRUE, TY_BOOL_FALSE, TY_INT_INTRO, TY_ELT_INTRO.
Similar to TY_UNIT_INTRO.

5 Additional Details

5.1 Well-formed types

$\boxed{\Theta \vdash f\ \mathsf{Cap}}$ Well-formed fractional capabilities

$$\frac{fc \in \Theta}{\Theta \vdash fc\ \mathsf{Cap}} \quad \text{WF\_CAP\_VAR}$$

$$\frac{}{\Theta \vdash 1\ \mathsf{Cap}} \quad \text{WF\_CAP\_ZERO}$$

$$\frac{\Theta \vdash f\ \mathsf{Cap}}{\Theta \vdash \frac{1}{2}f\ \mathsf{Cap}} \quad \text{WF\_CAP\_SUCC}$$

$\boxed{\Theta \vdash t\ \mathsf{Type}}$ Well-formed types

$$\frac{}{\Theta \vdash \mathbf{unit}\ \mathsf{Type}} \quad \text{WF\_TYPE\_UNIT}$$

$$\frac{}{\Theta \vdash \mathbf{bool}\ \mathsf{Type}} \quad \text{WF\_TYPE\_BOOL}$$

$$\frac{}{\Theta \vdash \mathbf{int}\ \mathsf{Type}} \quad \text{WF\_TYPE\_INT}$$

$$\frac{}{\Theta \vdash \mathbf{elt}\ \mathsf{Type}} \quad \text{WF\_TYPE\_ELT}$$

$$\frac{\Theta \vdash f\ \mathsf{Cap}}{\Theta \vdash f\ \mathbf{arr}\ \mathsf{Type}} \quad \text{WF\_TYPE\_ARRAY}$$

$$\frac{\Theta \vdash t\ \mathsf{Type}}{\Theta \vdash !t\ \mathsf{Type}} \quad \text{WF\_TYPE\_BANG}$$

$$\frac{\Theta, fc \vdash t\ \mathsf{Type}}{\Theta \vdash \forall fc.t\ \mathsf{Type}} \quad \text{WF\_TYPE\_GEN}$$

$$\frac{\begin{array}{l}\Theta \vdash t\ \mathsf{Type}\\ \Theta \vdash t'\ \mathsf{Type}\end{array}}{\Theta \vdash t \otimes t'\ \mathsf{Type}} \quad \text{WF\_TYPE\_PAIR}$$

$$\frac{\begin{array}{l}\Theta \vdash t\ \mathsf{Type}\\ \Theta \vdash t'\ \mathsf{Type}\end{array}}{\Theta \vdash t \multimap t'\ \mathsf{Type}} \quad \text{WF\_TYPE\_LOLLY}$$

5.2 Grammar Definition

m	::=		matrix expressions
	|	M	matrix variables
	|	$m + m'$	matrix addition
	|	$m\ m'$	matrix multiplication
	|	(m)	S

f	$::=$			fractional capability
	$\mid$	fc		variable
	$\mid$	1		whole capability
	$\mid$	$\frac{1}{2}f$		
t	$::=$			linear type
	$\mid$	**unit**		unit
	$\mid$	**bool**		boolean (true/false)
	$\mid$	**int**		63-bit integers
	$\mid$	**elt**		array element
	$\mid$	f **arr**		arrays
	$\mid$	f **mat**		matrices
	$\mid$	$!t$		multiple-use type
	$\mid$	$\forall fc.t$	bind fc in t	frac. cap. generalisation
	$\mid$	$t \otimes t'$		pair
	$\mid$	$t \multimap t'$		linear function
	$\mid$	(t)	S	parentheses
p	$::=$			primitive
	$\mid$	**not**		boolean negation
	$\mid$	$(+)$		integer addition
	$\mid$	$(-)$		integer subtraction
	$\mid$	$(*)$		integer multiplication
	$\mid$	$(/)$		integer division
	$\mid$	$(=)$		integer equality
	$\mid$	$(<)$		integer less-than
	$\mid$	$(+.)$		element addition
	$\mid$	$(-.)$		element subtraction
	$\mid$	$(*.)$		element multiplication
	$\mid$	$(/.)$		element division
	$\mid$	$(=.)$		element equality
	$\mid$	$(<.)$		element less-than
	$\mid$	**set**		array index assignment
	$\mid$	**get**		array indexing
	$\mid$	**share**		share array
	$\mid$	**unshare**		unshare array
	$\mid$	**free**		free arrary
	$\mid$	**array**		Owl: make array
	$\mid$	**copy**		Owl: copy array
	$\mid$	**sin**		Owl: map sine over array
	$\mid$	**hypot**		Owl: $x_i := \sqrt{x_i^2 + y_i^2}$
	$\mid$	**asum**		BLAS: $\sum_i \lvert x_i \rvert$
	$\mid$	**axpy**		BLAS: $x := \alpha x + y$
	$\mid$	**dot**		BLAS: $x \cdot y$
	$\mid$	**rotmg**		BLAS: see its docs
	$\mid$	**scal**		BLAS: $x := \alpha x$
	$\mid$	**amax**		BLAS: $\operatorname{argmax} i : x_i$
	$\mid$	**setM**		matrix index assignment

	$\vert$	**getM**		matrix indexing
	$\vert$	**shareM**		share matrix
	$\vert$	**unshareM**		unshare matrix
	$\vert$	**freeM**		free matrix
	$\vert$	**matrix**		Owl: make matrix
	$\vert$	**copyM**		Owl: copy matrix
	$\vert$	**copyM_to**		Owl: copy matrix onto another
	$\vert$	**sizeM**		dimension of matrix
	$\vert$	**trnsp**		transpose matrix
	$\vert$	**gemm**		BLAS: $C := \alpha A^{T?} B^{T?} + \beta C$
	$\vert$	**symm**		BLAS: $C := \alpha AB + \beta C$
	$\vert$	**posv**		BLAS: Cholesky decomp. and solve
	$\vert$	**potrs**		BLAS: solve with given Cholesky
	$\vert$	**syrk**		BLAS: $C := \alpha A^{T?} A^{T?} + \beta C$
v	$::=$			values
	$\vert$	p		primitives
	$\vert$	x		variable
	$\vert$	$()$		unit introduction
	$\vert$	**true**		true
	$\vert$	**false**		false
	$\vert$	k		integer
	$\vert$	l		heap location
	$\vert$	el		array element
	$\vert$	**Many** v		!-introduction
	$\vert$	**fun** $fc \to v$		frac. cap. abstraction
	$\vert$	$v[f]$		frac. cap. specialisation
	$\vert$	(v, v')		pair introduction
	$\vert$	**fun** $x : t \to e$	bind x in e	abstraction
	$\vert$	**fix** $(g, x : t, e : t')$	bind $g \cup x$ in e	fixpoint
	$\vert$	(v)	S	parentheses
e	$::=$			expression
	$\vert$	p		primitives
	$\vert$	x		variable
	$\vert$	**let** $x = e$ **in** e'	bind x in e'	let binding
	$\vert$	$()$		unit introduction
	$\vert$	**let** $() = e$ **in** e'		unit elimination
	$\vert$	**true**		true
	$\vert$	**false**		false
	$\vert$	**if** e **then** e_1 **else** e_2		if
	$\vert$	k		integer
	$\vert$	l		heap location
	$\vert$	el		array element
	$\vert$	**Many** e		!-introduction
	$\vert$	**let Many** $x = e$ **in** e'		!-elimination
	$\vert$	**fun** $fc \to e$		frac. cap. abstraction
	$\vert$	$e[f]$		frac. cap. specialisation

	$\|$	(e, e')		pair introduction
	$\|$	$\textbf{let}\,(a, b) = e\,\textbf{in}\,e'$	bind $a \cup b$ in e'	pair elimination
	$\|$	$\textbf{fun}\,x : t \to e$	bind x in e	abstraction
	$\|$	$e\ e'$		application
	$\|$	$\textbf{fix}\,(g, x : t, e : t')$	bind $g \cup x$ in e	fixpoint
	$\|$	(e)	S	parentheses
C	$::=$			evaluation contexts
	$\|$	$\textbf{let}\,x = [-]\,\textbf{in}\,e$	bind x in e	let binding
	$\|$	$\textbf{let}\,() = [-]\,\textbf{in}\,e$		unit elimination
	$\|$	$\textbf{if}\,[-]\,\textbf{then}\,e_1\,\textbf{else}\,e_2$		if
	$\|$	$\textbf{Many}\,[-]$		!-introduction
	$\|$	$\textbf{let}\,\textbf{Many}\,x = [-]\,\textbf{in}\,e$		!-elimination
	$\|$	$\textbf{fun}\,fc \to [-]$		frac. cap. abstraction
	$\|$	$[-][f]$		frac. cap. specialisation
	$\|$	$([-], e)$		pair introduction
	$\|$	$(v, [-])$		pair introduction
	$\|$	$\textbf{let}\,(a, b) = [-]\,\textbf{in}\,e$	bind $a \cup b$ in e	pair elimination
	$\|$	$[-]e$		application
	$\|$	$v[-]$		application
Θ	$::=$			fractional capability environment
	$\|$	$\cdot$		
	$\|$	Θ, fc		
Γ	$::=$			linear types environment
	$\|$	$\cdot$		
	$\|$	$\Gamma, x : t$		
	$\|$	Γ, Γ'		
Δ	$::=$			intuitionistic types environment
	$\|$	$\cdot$		
	$\|$	$\Delta, x : t$		
σ	$::=$			heap (multiset of triples)
	$\|$	$\{\}$		empty heap
	$\|$	$\sigma + \{l \mapsto_f m_{k_1,k_2}\}$		location l points to matrix m
$StepsTo$	$::=$			result of small step
	$\|$	$\langle \sigma, e \rangle$		heap and expression
	$\|$	$\textbf{err}$		error